07-06-05 / AF JW

PATENT

"EXPRESS MAIL" Mailing Label Number
ET694209159US

I HEREBY CERTIFY THAT THIS PAPER OR FEE IS BEING DEPOSITED WITH THE U.S. POSTAL SERVICE "EXPRESS MAIL POST OFFICE-TO-ADDRESSEE SERVICE" UNDER 37 CFR 1.10 ON THE DATE INDICATED BELOW AND IS ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450 ON:

5 July 2005
DATE OF DEPOSIT

SIGNATURE OF PERSON MAILING PAPER OR FEE

NAME OF PERSON SIGNING

Gary J. Pitzer 5 July 2005
DATE OF SIGNATURE

THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants	:	Vincent McCullough et al.
Serial No.	:	09/704,418
Filing Date	:	November 1, 2000
For	:	SYSTEM AND METHOD FOR EFFICIENT AND SECURE REVOCATION CERTIFICATION IN A PUBLIC KEY INFRASTRUCTURE
Group Art Unit	:	2131
Examiner	:	Taghi T. Arani, Ph.D.
Attorney Docket No.	:	NG(MS)7153

Mail Stop Appeal Briefs - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Sir:

Pursuant to the Notice of Appeal filed in this case on May 4, 2005, Appellants' present herewith their Brief on appeal.

07/08/2005 CCHAU1 00000004 200090 09704418
01 FC:1402 500.00 DA

I. REAL PARTY IN INTEREST

The real party in interest is Northrop-Grumman Corporation, as indicated by the Assignment recorded June 10, 2004, Reel/Frame: 013751/0849.

II. RELATED APPEAL AND INTERFERENCES

There are no related appeals or interferences.

III. STATUS OF CLAIMS

Claims 1, 2, 9-20, 23-25 and 28 stand rejected and are appealed.

Claims 3-8, 22, and 26-27 have been cancelled.

IV. STATUS OF AMENDMENTS

Claims 1, 9, 18-20, 23, 25 and 28 were amended and claims 8, 21- 22 and 26-27 were canceled in an amendment dated March 8, 2005. In particular, claim 1 was amended to incorporate dependent claim 8, claim 18 was amended to incorporate dependent claim 22 and claim 23 was amended to incorporate dependent claim 27. These amendments were entered for purposes of appeal according to an Advisory Action dated March 23, 2005.

Applicant also submits herewith an amendment to cancel claims 3-7. The cancellation of such claims does not affect the scope of any other pending claim in the proceedings, but is believed to help simplify issues on appeal.

V. SUMMARY OF THE CLAIMED SUBJECT MATTER

A. Summary of Independent Claim 1

Claim 1 is directed to a method for revocation of a signature certificate in a Public Key Infrastructure (PKI) (See Figure 4, and page 10, lines 1-3). A personal revocation authority (PRA) (144) is notified that a user has lost his/her user signature certificate (Page 17, lines 15-16; S32 of Figure 4). The PRA (144) may be one or more people that are in charge of revocation of members from the system, such as a manager or supervisor of the user (Page 13, lines 20-22; page 14, lines 17-20; page 17, lines 9-11). An authenticated secure channel is created with a registration web server (Page 17, lines 4-5; S36 of Figure 4, and 124 of Figure 2). The PRA (144) is notified that the user has lost his/her user signature certificate before the creation of the authenticated secure channel (Page 16, lines 19-21). The registration web server (124) is requested to revoke a user signature certificate (Page 17, lines 5-6, page 15, lines 19-20; S37 of Figure 4). The registration web server (124) is a software application that serves web pages (such as web page 122) or other HTML outputs to a web browser client (such as client 126) (Page 12, lines 5-9). The requesting to revoke the certificate occurs over the authenticated secure channel (Page 16, lines 1-2). The method also includes revoking the user signature certificate (Page 17, lines 13-15) and notifying a directory (108) by the registration web server (124) of revocation of the user signature certificate (Page 16, lines 3-4; page 17, lines 13-16; S41 of Figure 4, S17 of Figure 3) A user entry in the directory (108) is set to a state without a signature certificate (S41 of Figure 3; Page 17, lines 13-16).

B. Summary of claims depending from claim 1 and are being argued separately

Claim 9 further recites that the creating of the authenticated secured channel and the requesting of the registration web server to revoke are initiated by the personal revocation authority (Page 16, line 22, through page 17, line 6). The method of claim 10 includes requesting a personal registration authority's signature certificate to authenticate the personal registration authority before the creating (S37 of Figure 4; page 17, lines 5-6). Claim 11 recites that the PRA (144) is a supervisor of the user (Page 16, line 19-22; page 17, lines 9-11).

C. Summary of Independent Claim 18

Claim 18 is directed to a server (106) comprising a storage medium having instructions that can be executed for causing a processing device to perform a method. The method includes creating an authenticated secure channel is created with personal revocation authority (144) (Page 17, lines 4-5; S36 of Figure 4, and 124 of Figure 2). The PRA (144) may be one or more people that are in charge of revocation of members from the system, such as a manager or supervisor of the user (Page 13, lines 20-22; page 14, lines 17-20; page 17, lines 9-11). A request is received from the PRA to revoke a user certificate (S37 of Figure 4; page 17, lines 5-6). The user signature certificate is revoked (Page 17, lines 13-15) and a directory (108) is notified of revocation of the user signature certificate (Page 16, lines 3-4; page 17, lines 13-16; S41 of Figure 4, S17 of Figure 3).

D. Summary of Independent Claim 23

Claim 23 recites a system (100) for revocation of a signature certificate in a Public Key Infrastructure (PKI) (See Figure 4, and page 10, lines 1-3). The system (100) includes at least one server (106) that is operably connected to a network (Page 10, lines 4-6). A directory (108) is operably connected to the network and the directory (108) contains information on at least one user (Page 10, line 20, through page 11, line 4). At least one client platform (128), such as any user computer or computing device, is operably connected to the network to provide the at least one user access to the at least one server from the client platform (Page 12, lines 10-21). A registration web server (124) is operably connected to the network. The registration web server (124) is a software application that serves web pages (such as web page 122) or other HTML outputs to a web browser client (such as client 126) (Page 12, lines 5-9). The registration web server (124) receives a request for revocation of a user signature certificate from a personal revocation authority (144) (Page 14, line 17, through page 15, line 1). The PRA (144) may be one or more people that are in charge of revocation of members from the system, such as a manager or supervisor of the user (Page 13, lines 20-22; page 14, lines 17-20; page 17, lines 9-11). The registration web server (124) revokes the user signature certificate only if the personal revocation authority (144) is permitted to revoke the user signature certificate (S39 of Figure 4, page 17, lines 13-18; page 14, line 17, through page 15, line 1). The registration web server (124) notifies the directory (108) of revocation of the user signature certificate if revoked (S41 of Figure 4, page 17, lines 13-16).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1 (original claim 8) and claim 23 (original claim 27) stand rejected under 35 U.S.C. 103(a) as being obvious by U.S. Patent No. 6,134,328 (hereinafter "Cordery") in view of U.S. Pub. No. 2001/0011255 A1 (hereinafter "Asay").

2. Claim 18 (original claim 22) stands rejected under 35 U.S.C. 103(a) as being obvious by Cordery in view of U.S. Patent 6,715,073 (hereinafter "An et al.").

3. Claims 9 and 11 stand rejected under 35 U.S.C. 103(a) as being obvious by Cordery in view of Asay in view of in further view of An et al.

VII. ARGUMENT

1. Independent claims 1 and 23 stand rejected under 35 U.S.C. 103(a) as being made obvious by Cordery in view of Asay.

The Board of Patent Appeals and Interferences has held that, "to support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." *Ex parte Clapp*, 227 U.S.P.Q. 972, 973 (Bd. Pat App. & Inter. 1985).

i. **Claim 1** - Cordery and Asay, taken alone or in combination do not teach or suggest notifying a personal revocation authority (PRA) that a user has lost a user signature certificate before creating an authenticated secure channel with a registration web server.

Claim 1 is patentable over Cordery in view of Asay because: (i.) Cordery and Asay, taken alone or in combination do not teach or suggest notifying a personal revocation

authority (PRA) that a user has lost a user signature certificate before creating an authenticated secure channel with a registration web server.

The Final Office Action dated January 6, 2005 (hereinafter "Final Office Action"), states that "Cordery's certificate management device inherently carries output the recited steps and functionality of a registration web server." Office Action dated January 6, 2005, at page 3, lines 3-4. It is well settled that a limitation is inherently disclosed by a reference only if it is necessarily present and a person of ordinary skill in the art would recognize its presence. *Crown Operations Int'l Ltd. v. Solutia Inc.*, 289 F.3d 1367, 1377, 62 U.S.P.Q.2d 1917, 1922-1923 (Fed. Cir. 2002). Applicant's patent application states that the registration web server (124) is a software application that serves web pages (such as web page 122) or other HTML outputs to a web browser client (such as client 126). Applicant's patent application at page 12, lines 5-9. In contrast, Cordery fails to teach any creation of a secure channel with a registration web server, a recited in claim 1. Instead, the only secure communications disclosed in Cordery occur between a personal computer (204) and a postage meter (218) over a direct link or between the PC (204) and a remote facility (222) via a modem (220). See Figure 2 of Cordery; Col. 4, line 60, through Col. 5, line 1. Cordery describes that the communication with the remote facility (222) can be by way of hardwire or can be by way of radio frequency communication or other communications. Cordery at Col. 5, lines 5-8. Moreover, nothing in the method described in Figure 6 of Cordery supports the contention that a registration web server is employed in a secure channel. Additionally, the description of the method of Figure 6 in Cordery, especially at step 604, is silent as to what type of hardware and/or software might be employed to verify the request.

The Court of Appeals for the Federal Circuit has mandated that inherency may not be established by probabilities or possibilities. *Crown Operations Int'l Ltd. v. Solutia Inc.*, supra., at 1923. The mere fact that a certain thing may result from a given set of circumstances is not sufficient. *Id.* As stated above, Cordery provides no teaching (or even a suggestion) that any communication, including a request to a certificate authority is provided as a request to a registration web server over the authenticated secure channel, as recited in claim 1. One of ordinary skill in the art would not recognize that the secure communication described with respect to Figures 2 and 6 of Cordery necessarily are with a registration web server because no mention of a web server or the Internet is provided in Cordery, whereas other direct communication methods are disclosed in Cordery.

Since Cordery fails to disclose use of a registration web server, Cordery similarly fails to teach any requesting of the registration web server to revoke a user signature certificate, as recited in claim 1. The Office Action also relies on 608 of FIG. 6 for issuing a singed message to postage and certificate meter to revoke the certificate. However, the signed message being issued in connection with step 608 of Cordery does not disclose that the signed message be sent to a registration web server, but instead Cordery teaches that the signed message is sent to a postage meter subsystem 218. See Cordery at Col. 8, lines 16-19. Nothing in Cordery teaches or suggests that the postage meter could be a web server.

Significantly, the Final Office Action admits that Cordery does not teach notifying a PRA by a user that the user has lost the user signature certificate, the notifying occurring before the creating. The Final Office Action at page 8, lines 1-2. The Final Office Action, at page 8, lines 3-9, cites Asay in an effort to cure the above-mentioned deficiencies of Cordery

in support of its rejection of claim 8, which has been incorporated by amendment into claim 1. In pertinent part, Asay states that:

> "A subscriber can revoke a certificate to prevent reliance on forged digital signatures created using a compromised, e.g., lost or stolen, private key" (See Asay, Para. [0014]).

Asay does not teach or suggest a anyone, and particularly a PRA, being notified that the certificate has been compromised. In the present application, a PRA is described as a one or more people that are in charge of revocation of members from a system network. See the present application page 13, lines 20-22; page 14, lines 17-20; page 17, lines 9-11. Since the PRA of claim 1 is one or more people, claim 1 thus recites two different people for use in performing the method recited therein, namely, a user and a PRA. The subscriber disclosed in Cordery cannot be seen as corresponding to two different people.

Moreover, Cordery fails to expressly or impliedly teach that a subscriber would notify a PRA that a signature certificate has been lost. In contrast, in Asay et al., its is the subscriber can revoke his/her own certificate. See Asay et al. paragraph [0014]. Asay et al. fails to teach or suggest a user notifying a PRA that the user has lost his/her signature certificate so that the PRA can request revocation of the signature certificate. Applicant submits that Asay et al. emphasizes facilitating digital transactions with automatic services. See generally Asay et al. at paragraphs [0021]-[0027]. The Court of Customs and Patent Appeals has held that if the proposed modification or combination of the prior art would change the principle operation of the prior art invention being modified, then the teachings of the references are not sufficient to render the claims prima facie obvious. *In re Ratti*, 270 F.2d 810, 123 U.S.P.Q. 349 (CCPA 1959). Modifying Asay in the manner suggested above would require an additionally step (notifying a PRA) that would impose a substantial burden on the revocation process disclosed

in Asay. As mentioned above, nothing in Asay would teach or suggest increasing human involvement during the revocation process. Thus, Asay does not provide a teaching from which one of ordinary skill in the art would discern the capability to notify a PRA that a user has lost a user signature certificate, which notification occurs before creating an authenticated secure channel with a registration web server, as recited in claim 1. Accordingly, it would not have been obvious to modify Asay to require a subscriber notify a PRA to revoke a certificate.

Furthermore, it is respectfully submitted that one of ordinary skill in the art would not look to combine and modify Cordery in view of Asay in the manner suggested by the Office Action. It is well established law that an Examiner may not use the patent application as a basis for motivation to combine or modify the prior art to arrive at the claimed invention. *In re Dow Chem. Co.*, 837 F.2d 469, 473, 5 U.S.P.Q.2d 1529, 1531 (Fed. Cir. 1988). Cordery discloses a system and method for allowing a postal service to employ a certificate authority (CA), such as the post office or other trusted third party, to provide universal access to a postage meter system. See Cordery at Col. 3, line 49, through Col. 4, line 5. Thus, a postal service employing the system disclosed in Cordery relies on the automatic verification of the certificate purported by certificate authority. Cordery at Col. 6, lines 54-63. Nothing in Cordery would teach or suggest the increasing of human involvement during the revocation of a certificate, as is suggested in the Final Office Action. In rejecting the present application, it appears that the Office is impermissibly using the present application as the motivation (by providing a missing teaching) to increase human involvement in the revocation process. See *Arkie Lures Inc. v. Gene Larew Tackle Inc.*, 119 F.3d 953, 43 U.S.P.Q.2d 1294, 1297 (Fed. Cir. 1997).

For the reasons stated above, it is respectfully suggested that the rejection of claim 1 is improper and should be withdrawn.

ii. Claim 23 - Cordery and Asay, taken alone or in combination do not teach or suggest a registration web server operably connected to a network, the registration web server receiving a request for revocation of a user signature certificate from a PRA, the registration web server revoking the user signature certificate only if the PRA is permitted to revoke the user signature certificate.

Claim 23 is patentable over Cordery in view of Asay because: Cordery and Asay, taken alone or in combination do not teach or suggest a registration web server operably connected to a network, the registration web server receiving a request for revocation of a user signature certificate from a PRA, the registration web server revoking the user signature certificate only if the PRA is permitted to revoke the user signature certificate.

Cordery does not teach or suggest a registration web server receiving a request for revocation of a user signature certificate from a PRA, the registration web server revoking the user signature certificate only if the PRA is permitted to revoke the user signature certificate.

The addition of Asay does not cure the deficiencies of Cordery. As stated above with regard to claim 1, Asay does not teach or suggest the use of a PRA as recited in claim 23. Furthermore, as also stated with regard to claim 1, Cordery and Asay there is insufficient motivation to combine Cordery and Asay et al. in the manner suggested in the Office Action. Thus, Cordery and Asay do not make claim 23 obvious. Accordingly, it is respectfully suggested that the rejection of claim 23 is improper and should be withdrawn.

2. Independent claim 18 stands rejected under 35 U.S.C. 103(a) as being obvious by Cordery in view of An et al.

i. Cordery and An et al. taken alone or in combination do not teach or suggest creating an authenticated secure channel between a server a PRA and receiving a request from the PRA to revoke a user signature certificate.

Claim 18 is patentable over Cordery in view of An et al. because: (i.) Cordery and An et al. taken alone or in combination do not teach or suggest creating an authenticated secure channel between a server a PRA and receiving a request from the PRA to revoke a user signature certificate.

The Final Office Action admits that Cordery does not teach a PRA. See Final Office Action, at page 15, lines 7-11. In the present application, a PRA is described as a one or more people that are in charge of revocation of members from a system network. See Applicant's present application page 13, lines 20-22; page 14, lines 17-20; page 17, lines 9-11. Thus, it is clear that the PRA of claim 18 is one or more people, not a software process. See the present application at page 16, lines 21-22.

The Final Office Action relies on the teachings of An et al. to cure the deficiencies of Cordery. In pertinent part, An et al. states that:

> "A registration authority running as a software application in the controller processes requests to issue, renew and revoke digital certificates issued by a certification authority using two pairs of public-private keys." See Abstract of An et al.

For example, the registration authority 20 is an SSL-enabled web browser. See Figure 1 of An et al. An et al. thus teaches that the registration authority is software and not a person.

In regards to Figure 4, An et al. further discloses a web server that interacts with a supervisor, which includes a request supervisor 32^1, a communication supervisor 32^2, and service supervisor 32^3 where each supervisor provides a different service for the vaults." An et al. at Col. 8, lines 20-24. In rejecting claims 11 and 28, the Final Office Action contends that such supervisors 32^1, 32^2, and 32^3 correspond to a supervisor of the user. One of ordinary

skill in the art, however, would not recognize any such supervisor as being a person based on the teachings of An et al., since each of the supervisors 32^1, 32^2, 32^3 are depicted and described as being implemented as software services running on a trusted computer base. See Figure 4 and Col. 8, lines 20-32 of An et al. Thus, An et al. fails to teach or suggest the use of a personal revocation authority, as recited in claim 18.

Since the registration authority disclosed in An, et al. is not a personal revocation authority, as recited in claim 18, Cordery and An, et al., taken individually or in combination, do not teach or suggest claim 18. For these reasons, Applicant respectfully requests that the rejection of claim 18 be withdrawn.

3. Claims 9 and 11 stand rejected under 35 U.S.C. 103(a) as being obvious by Cordery in view of Asay in view of in further view of An et al.

The Board of Patent Appeals and Interferences has held that, "to support the conclusion that the claimed combination is directed to obvious subject matter, either the references must expressly or impliedly suggest the claimed combination or the examiner must present a convincing line of reasoning as to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references." Ex parte Clapp, 277 U.S.P.Q. 972, 973 (Bd. Pat App. & Inter. 1985).

i. Claim 9- Cordery, Asay and An et al. taken alone or in combination do not teach or suggest that the creating and requesting are initiated by a personal revocation authority.

Claim 9 is patentable over Cordery in view of Asay in further view of An et al. because Cordery, Asay and An et al., taken alone or in combination, do not teach or suggest that the creation of an authenticated secure channel and the requesting of the registration web server are initiated by a personal revocation authority (PRA).

Claim 9 depends from claim 1 and is patentable for at least the same reasons as claim 1. The Final Office Action admits that Cordery in view of Asay does not teach that creating and requesting are initiated by a PRA. Final Office Action at page 8, last paragraph. The Final Office Action cites An et al. in an effort to cure the above deficiencies of Cordery in view of Asay. As mentioned above with respect to claim 18, An et al. discloses a registration authority that runs as software. Clearly, software is not a person. Moreover, nothing in An et al. suggests that the registration authority both initiates the creation of an authenticated secure channel and requests that the registration web server revoke a user signature certificate. Instead, the registration authority reviews and approves requests initiated from an applicant, namely a user. An et al. at Col. 6, lines 15-34, Col. 10, lines 40-57. The applicant then generates a public-private key pair and sends the public key to the certification authority. An et al. at Col. 10, line 65, through Col. 11, line 3. Thus, An et al. teaches that it is the user and the registration authority that creates the authenticated secure channel and initiates the request. For these reasons, Cordery in view of Asay, in further view of An et al. does not make claim 9 obvious. Accordingly, it is respectfully requested that the rejection of claim 9 should be withdrawn.

ii. Claim 11 - Cordery Asay and An et al. taken alone or in combination do not teach or suggest PRA that is the supervisor of a user.

Claim 11 is patentable over Cordery in view of Asay in further view of An et al. because: (i.) Cordery, Asay and An et al. taken alone or in combination do not teach or suggest PRA that is the supervisor of a user.

Claim 11 depends indirectly from claim 9 and is patentable for at least the same reasons as claim 9. Moreover, as stated above with respect to claim 9, An et al. discloses a registration authority running as software. Since software is not a person, the registration authority disclosed in An et al. is not a supervisor of a user. The Final Office Action contends that the personal registration authority is a supervisor of the user by referring to Figure 4 and Col. 5, lines 7-13. Final Office Action at page 9, lines 14-15. However, the supervisors of Figure 4 correspond to distinct supervisory software processes 32^1, 32^2, 32^3 that are depicted and described as being implemented as software services running on a trusted computer base. See Figure 4 and Col. 8, lines 20-32 of An et al. Thus, An et al. fails to teach or suggest the use of a personal revocation authority, as recited in claim 18. For these reasons, Cordery in view of Asay, in further view of An et al. do not make claim 11 obvious. Accordingly, it is respectfully suggested that the rejection of claim 11 be withdrawn.

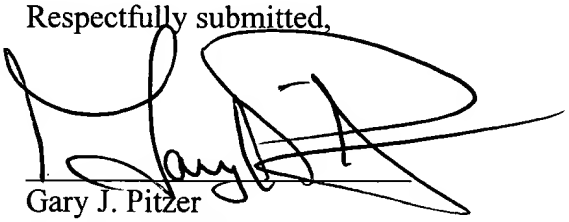
VIII. APPENDIX

The attached Claims Appendix contains a copy of the claims on appeal.

An Amendment After Appeal is also submitted herewith.

Please charge any deficiency or credit any overpayment in the fees for this Appeal Brief to Deposit Account No. 20-0090.

Respectfully submitted,



Gary J. Pitzer
Reg. No. 39,334

TAROLLI, SUNDHEIM, COVELL
& TUMMINO, L.L.P.
526 Superior Avenue – Suite 1111
Cleveland, Ohio 44114
(216) 621-2234
(216) 621-4072 (Facsimile)
Customer No.: 26294

Sinda

Claims Appendix

Claim 1 A method for revocation of a signature certificate in a Public Key Infrastructure (PKI) comprising:

creating an authenticated secure channel with a registration web server;

requesting the registration web server revoke a user signature certificate, the requesting occurring over the authenticated secure channel;

revoking the user signature certificate;

notifying a directory by the registration web server of revocation of the user signature certificate;

setting a user entry in the directory to a state without a signature certificate; and

notifying a personal revocation authority that a user has lost a user signature certificate, the notifying occurring before the creating.

Claim 2 The method according to claim 1, further comprising generating a directory password for the user during creation of the user signature certificate.

Claim 7 The method according to claim 3, further comprising using the user signature certificate to authenticate the user before the creating.

Claim 9 The method according to claim 1, wherein the creating and requesting are initiated by the personal registration authority.

Claim 10 The method according to claim 9, further comprising requesting a personal registration authority's signature certificate to authenticate the personal registration authority before the creating.

Claim 11 The method according to claim 10, wherein the personal registration authority is a supervisor of the user.

Claim 12 The method according to claim 10, further comprising querying the directory after the requesting the registration web server revoke the user signature certificate to determine if the personal registration authority is permitted to revoke the user signature certificate.

Claim 13 The method according to claim 12, further comprising revoking the user signature certificate by the registration web server only if the personal registration authority is permitted to revoke the user signature certificate.

Claim 14 The method according to claim 13, further comprising generating a directory password for the user during creation of the user signature certificate.

Claim 15 The method according to claim 14, further comprising sending the user one of a password and a personal identification number (PIN) by the registration web server after the setting of the user entry.

Claim 16 The method according to claim 15, further comprising requesting a new signature certificate by the user using the directory password and one of the password and the PIN.

Claim 17 The method according to claim 1, wherein the revoking is performed by the registration web server.

Claim 18 A server comprising a storage medium having instructions stored therein, the instructions when executed causing a processing device to perform:

creating an authenticated secure channel between the server and a personal registration authority;

receiving a request from the personal revocation authority to revoke a user signature certificate;

revoking the user signature certificate; and

notifying a directory of revocation of the user signature certificate.

Claim 19 The server according to claim 18, further comprising verifying the personal registration authority is permitted to revoke the user signature certificate.

Claim 20 The server according to claim 19, further comprising revoking the user signature certificate only if the personal registration authority is permitted to revoke the user signature certificate.

Claim 23 A system for revocation of a signature certificate in a Public Key Infrastructure (PKI) comprising:

at least one server operably connected to a network;

a directory operably connected to the network, the directory containing information on at least one user;

at least one client platform operably connected to the network, the at least one user having access to the at least one server from the at least one client platform; and

a registration web server operably connected to the network, the registration web server receiving a request for revocation of a user signature certificate from a personal revocation authority, the registration web server revoking the user signature certificate only if the personal revocation authority is permitted to revoke the user signature certificate, the registration web server notifying the directory of revocation of the user signature certificate if revoked.

Claim 24 The system according to claim 23, wherein the information on at least one user includes a user entry related to the user signature certificate, the directory setting the user entry in the directory to a state without a signature certificate if the user signature certificate is revoked.

Claim 25 The system according to claim 23, further comprising an authenticated secure channel between the personal registration authority and the registration web server, the requesting occurring over the authenticated secure channel.

Claim 28 The system according to claim 23, wherein the personal registration authority is a supervisor of the at least one user.